Alpha and Omega

The security shift from beginning to the endpoint

Orange
Cyberdefense

About us

“The Orange Cyberdefense Security Research Centre (SRC), is a specialist security research unit within the group that helps us fulfill our mission of being a trusted partner to our customers by ensuring that we identify, track, analyse, communicate and act upon significant developments in the security landscape that may impact them. Our team of dedicated researchers is globally recognised and frequently showcased at international security events and in leading publications. Their exceptional skills and unrivaled experience impact directly on our operations and are made accessible to our clients in various forms across our range of products and services”.

Charl van der Walt
Head of Security Research
Orange Cyberdefense

Introduction

Over the past two decades, the enterprise has evolved significantly in terms of technology, software and connectivity. However, one aspect remains pretty constant: the importance of the employee workstation and desktop PC or laptop. The proliferation of these endpoints across an enterprise network will continue for the foreseeable future, despite some workforces growing more mobile.

As such, these endpoints will remain key targets for hackers wanting to gain access to an organisation's network and data – be they external actors, or threats originating from within the organisation itself.

The weakest security link for a company is often its own employees: according to the UK government, phishing is the most common cause of breaches for UK businesses (identified by 80% of companies that have experienced breaches), followed by others impersonating an organisation in emails or online (28%) and viruses, spyware or malware (27%). All are the result of human activity.

The growing attack-surface presented by a desktop, its value in terms of data and as a foothold, and the exasperating role played by the user have made the endpoint an increasingly popular target. This has dramatically altered the network security paradigm. Where once it was sufficient to protect only the perimeter of a corporate network, this outdated approach is now no longer enough. Instead there must be a new, comprehensive and ongoing focus on endpoint security.

This whitepaper looks at the need for effective monitoring of endpoints and the challenges involved in choosing, deploying and managing an effective endpoint monitoring capability.

It then considers how some of these can be addressed by outsourcing security to a managed services provider.

Why desktop tops the target list

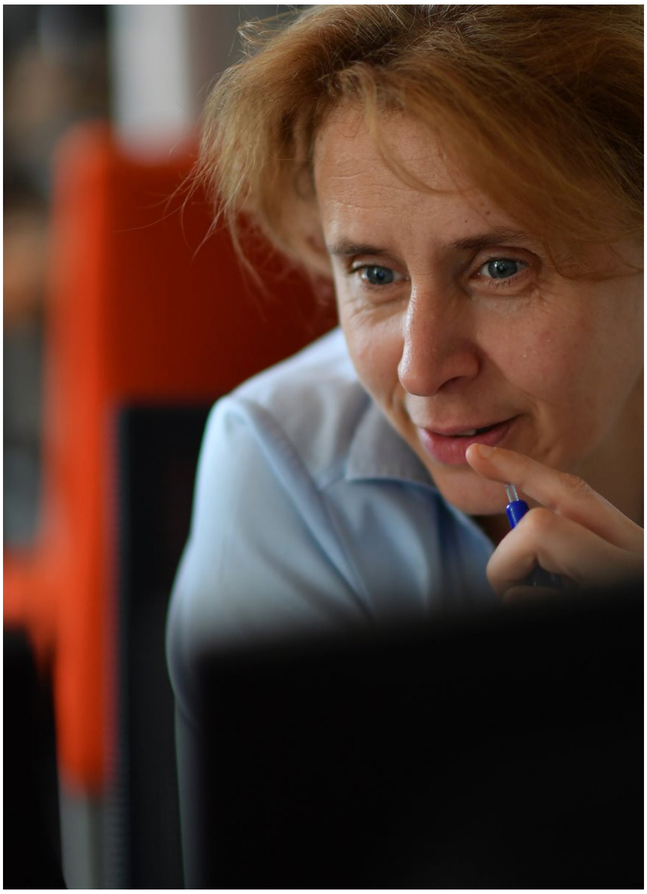
The desktop PC or laptop at a workstation is a popular and effective target for hackers. Why? Because the desktop effectively is the user in a modern network: gain access via this endpoint and you gain access to user data, domain credentials, user location, video and audio, as well as inherited privileges on other systems.

The desktop also offers a foothold into exploiting an enterprise's wider network: it provides the ideal location for lateral movement and pivoting, offers up numerous channels for exfiltration, and is hard for organisations to effectively monitor.

Plus, this endpoint is directly accessible from the internet (albeit via user activity), making the desktop a soft target which shows no sign of disappearing from the enterprise workplace any time soon.

> **Hackers are now far more likely to target Microsoft Office than web browsers, according to a 2018 report.**

Finally, for many enterprises, the desktop equates to Microsoft. It's widespread use and central role in many organisations has led hackers to develop and constantly evolve techniques to exploit vulnerabilities in Microsoft and its supported applications. Hackers are now far more likely to target Microsoft Office than web browsers, according to a 2018 report, which found that 47% of users were attacked via Office, a huge jump from the 16% recorded in 2016.



Microsoft Under Attack: Then and Now

Then

In 2017, Orange Cyberdefense's Attack and Penetration Testing division - SensePost - published a blog identifying how Microsoft Word's Dynamic Data Exchange (DDE) feature could be exploited to distribute malware, bypassing macro filtering email gateways and corporate VBA policies.

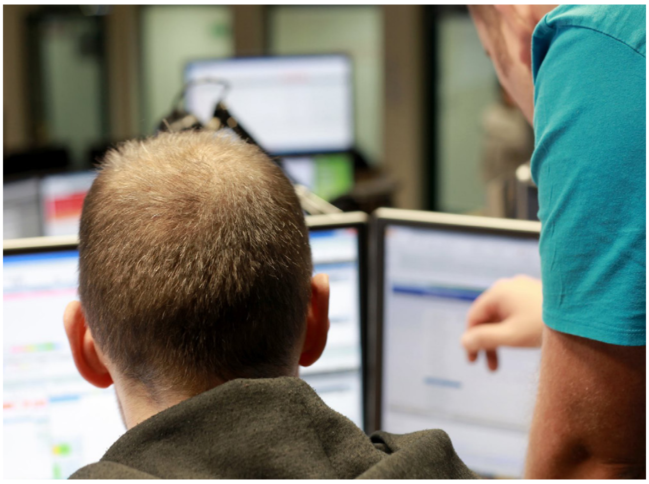
Microsoft initially denied the problem, calling it a 'feature' not a bug, before introducing a 'workaround' and offering advice on mitigating attacks via DDE. This included not opening suspicious email attachments – something which should be basic security policy in all organisations – and manually creating and setting registry entries for Office.

In the end, Microsoft was forced to release what it termed a 'patch', but which was actually an update that just disabled the DDE feature in Office applications.

Now

In June this year, Microsoft was forced to release another warning, this time regarding an active spam campaign that could infect users who simply open a document attached to an email. This attachment is in Rich Text Format and, when opened by Windows, targets the Equation Editor vulnerability CVE-2017-11882 to launch a malicious payload.

Although the campaign targeted primarily European users, the same vulnerability has in the past been used by Chinese cyber-espionage groups, and was identified as one of the most popular targeted vulnerabilities of 2018.



Let's start with the endpoint

Today, most organisations must manage and secure hugely complex IT infrastructures which are agile, and can be scaled rapidly. Such deep, widespread, multifaceted architectures present the malicious actor with an extremely broad attack surface and render the concept of network perimeter security almost laughable.

The traditional approach of simply using firewalls to protect an enterprise network is akin to protecting the crown jewels with a garden fence. Hackers can jump over, go through and break down these defences by exploiting endpoints and externally exposed services and applications. To achieve the robust protection that is needed, businesses must move away from the idea of perimeter security, and instead start any new security strategy with endpoint security in mind. US giant Google pivoted very boldly to an endpoint-centric approach to security with their 'Beyondcorp' initiative after they themselves became the victims of a Chinese campaign known as Aurora. The campaign in question successfully compromised endpoints within their network by targeting Internet Explorer vulnerabilities.

Those still taking the traditional perimeter security approach will likely neglect the importance of effectively managing and securing endpoints. In fact, a recent survey of 1,000 IT professionals found that, while 88% acknowledge the importance of endpoint management, almost a third are completely in the dark as to how many endpoints actually exist within their company. Furthermore, only around half are proactively addressing security concerns. This 'wait and see (and hope!)' approach in today's reality is irresponsible and significantly ups a business' chances of financial and reputational damage.

One critical component of an endpoint security strategy is visibility – the use of telemetry to understand what's happening on an endpoint, detect anomalous or malicious behaviours and identify and disrupt attacks before they can cause real damage. Endpoint telemetry at scale is tricky, but there are four general strategies being deployed by mature businesses to achieve it:

1. **Endpoint Protection, Detection and Response (EDP/R)**, also sometimes known as 'Next Generation' anti-virus, relies on the deployment of software agents to the endpoint to detect and contain attacks.

2. **Network monitoring** relies on traffic analysis and deep-packet inspection to deduce what's happening on the endpoint.

3. **User and Entity Behaviour Analytics (UEBA)** works by baselining user activity and behaviour to detect potential intrusions and malicious activity.

4. **Security Incident and Event Management (SIEM)** systems collect log data and other intelligence from a myriad of systems (including EDDP, Network, UEBA and others) and correlate them to allow operators to manually or automatically detect indicators of attack and compromise.

Driven in part by Silicon Valley marketing savvy and in part by the growing belief in Machine Learning, EDP/R approaches are enjoying high levels of popularity right now.

Detection Strategies: Risk vs Attack Surface

When enterprises deploy cybersecurity technologies, they face a dilemma: on the one hand the introduction of these tools to a network can help mitigate risk, but on the other, enterprises are simply increasing the attack surface and potentially upping their level of vulnerability.

This is particularly true for anti-virus or agent-based endpoint protection solutions. Using these (or only these) as the basis of an endpoint telemetry strategy is ineffective for a number of reasons:

- Agent-based solutions use complex code that has to process unfiltered data from untrusted sources, increasing the size of the attack surface, especially if this code is written by an unproven or inexperienced solutions provider
- Agent-based solutions are usually designed to detect anomalous software and not 'living off the land' (LOTL) techniques, which avoid injecting code into the victim and look almost indistinguishable from regular user activity
- Lumping protection and detection into a single solution is counterintuitive – we need detection because we assume protection has failed

A different approach is needed

Gaining decent visibility into activities of a Windows endpoint (both the workstation and the server) is critical. To defend endpoints for companies large and small, this approach needs to be affordable and straightforward. One tool which can play a key role in this approach is Microsoft Sysmon.

This Microsoft-native technology offers enterprises highly granular telemetry on its Windows endpoints, and is a remarkably powerful tool:

- It's standard Microsoft technology, meaning there are no third-party technology integration issues to solve, or code to manage
- It looks at behaviour rather than malware and can detect a wide range of threats targeted at the endpoint, including the whole gambit of 'LOTL (Living off the Land) attacks
- It enjoys widespread adoption by a growing community that collaborates to build valuable rules and filters
- It's free and easily accessible.

However Sysmon, as with all tools, needs to be fine-tuned to deliver effective real-time visibility into the Windows endpoint environment. The log collection, normalisation and analysis associated with this kind of solution are complex, skills-dependent and resource-intensive tasks, which many organisations will struggle to manage alone As such, many include it as part of a managed services approach (more on this later).

Let's start with the endpoint

What exactly are the biggest threats companies and their employees face? Perhaps unsurprisingly, phishing is the mostcommon weapon wielded by hackers, with 93% of data breaches attributed to phishing attacks, according to a 2018 Verizon report.

Cyber-attack: Common methods

Spearphishing:

What?

A targeted attack in which a hacker poses as an employee using a spoofed email address, bypasses antivirus software, and contacts another member(s) of the workforce to encourage them to divulge sensitive data or information.

When?

FireEye recently unearthed a highprofile incidence of spearphishing, in which Russian state-sponsored groups targeted European government organisations, sending emails to individuals which appeared to be from a genuine sender, and appeared to link to a genuine government website. Recipients were encouraged to change their password via a link, resulting in them unwittingly sharing their credentials with the attacker.

Credential stuffing:

What?

Hackers use a large database of usernames and passwords obtained from a previous data breach, and then use these to gain access to other online platforms. Employees have made things pretty easy for hackers: according to research by Dashlane, a worrying 52% of people use the same password (or very similar) to access various services across personal and work accounts.

When?

In 2016, a BBC investigation discovered that hackers had gained unauthorised access to the accounts of Deliveroo customers, ordering thousands of pounds worth of food deliveries with users' payment details. Credential stuffing was to blame, with Deliveroo commenting at the time that the criminals had used passwords "stolen from another service unrelated to our company in a major data breach."

Applications under attack:

What?

Applications are the lifeblood of most businesses and are no longer only accessed by employees using on-premise hardware; they're available on mobile, laptop, tablet, over public or private Wi-Fi, globally. This has provided another source of network entry for hackers, compounded by the fact that security vulnerabilities have been found in many business-critical applications.

When?

Perhaps the most infamous cybersecurity disaster of recent years, the attack on credit bureau Equifax was attributed to an online application vulnerability which was exploited by hackers. Social security numbers, addresses, dates of birth, and in some cases driver's license numbers, were exposed, affecting almost 148 million people.

Fortunately, many of us are wising up to phishing scams – click rates in phishing exercises fell from a high of around 25% in 2012, to around 3% in 2019, according to Verizon. But threats – spyware, malware, ransomware, viruses, both internal and external – will never disappear. As such, businesses must take a proactive approach to security, and effectively prepare themselves accordingly.

Time poor, resource poor

Aside from the inescapable fact that cyber-attacks are themselves inescapable, another challenge looms large over many organisations: the lack of specialist skills, IT resources and time required to secure a business' network, and all associated endpoints. The skills required for security have become both deeper and broader, the market more competitive and of course the earnings expectations of these specialists more demanding.

Plus, being a hacker isn't a 9-to-5 job, leaving many businesses vulnerable when IT teams clock off. Specialist skills and 24x7x365 monitoring and support are required, but lacking in many cases. Almost 40% of respondents to a 2019 EY survey, for example, said that less than 2% of their total IT headcount work in security. The same report found that over half of organisations had no programme in place – or else had an obsolete one – to cover areas such as threat intelligence, breach detection and data protection.

The latter is particularly concerning considering that GDPR was implemented back in May 2018. The ICO initially claimed that maximum fines for organisations found to have breached regulations would not be the norm, however, it has increased financial penalties by more than £1 million over the past year. Just recently, it was reported that British Airways is now facing a record £183m in fines as a result of last year's data breach, affecting 500,000 customers. The ICO's warnings are becoming a stark reality for those businesses who neglect the security and privacy of their customers' personal information.

Effective endpoint monitoring is needed to ensure organisations protect themselves, their customers, partners and third parties, and avoid fines by adhering to GDPR. This must involve incident response, malicious code detection and prevention, platform integrity and application sandboxing, application whitelisting, patching, updates and upgrades – and a lot more. The increase in the use of Living of the Land (LOTL) techniques by hackers, for example, makes attacks more difficult to detect than traditional approaches of loading a trojan or backdoor. This is a lot for an in-house team to take on, and, with insurance provider Hiscox ranking almost three-quarters of businesses as 'cyber novices', in many cases an impossible task.

With internal IT teams stretched, organisations could instead look for external assistance, from specialists inendpoint management and network security, and teams who are able to provide continuous, effective support.

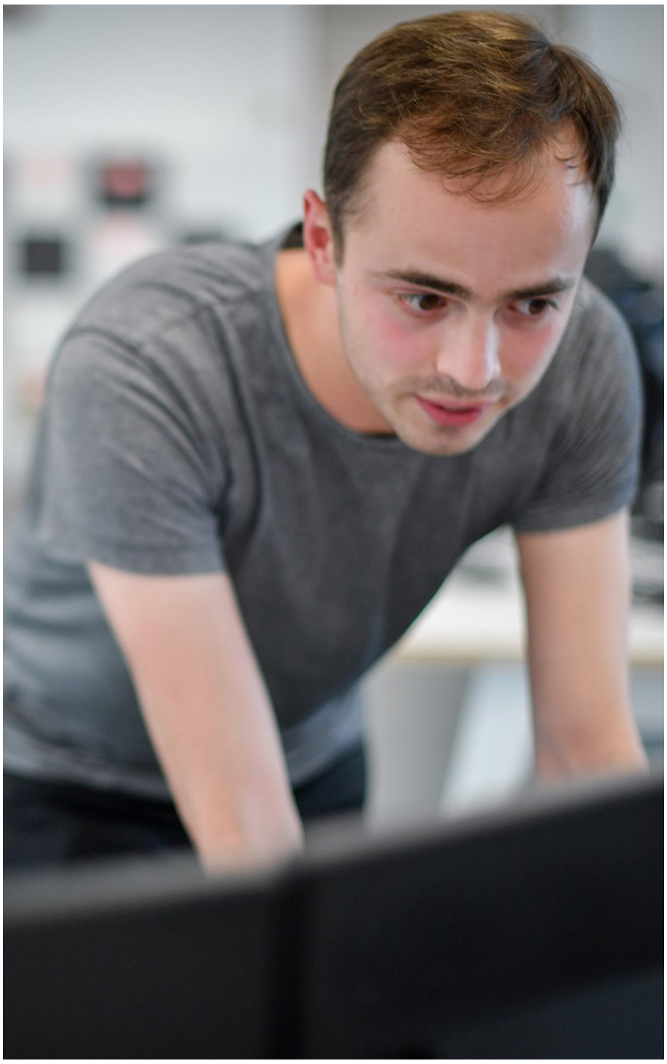
The managed service approach

The past two decades have seen many applications and operational services shift from being costly, cumbersome, on-premise and quickly out dated, to being available as-a-service; outsourced and managed by a specialist third party. Contracts are flexible, updates are frequent, and having an external resource dedicated to a single function frees up internal teams to focus on department - or business-critical functions.

The same is now available for an organisation's cybersecurity. Orange Cyberdefense offers a Managed Next-Generation Endpoint Security service, designed to provide 24x7x365 management, monitoring, support and systemhealth alerting across devices on a business' supported device list. Costs are transparent, and adaptable to the size, financial resources and scale of protection a business requires.

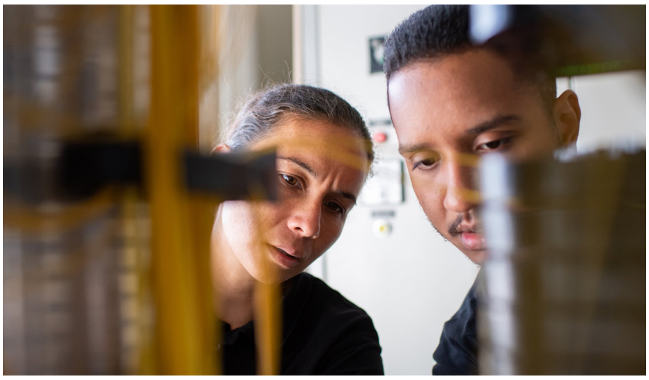
The benefits of effective management of a business' network and endpoint estate include:

- Helping to safeguard business critical assets
- Maintaining regulatory compliance
- Minimising the risk of ransomware attack and data theft
- Enabling visibility into device and user behaviour



Our service is composed of a number of components, including:

1. **A dedicated Security Expert** who serves as single point of contact without invoking the cost of an in-house team of cybersecurity practitioners and analysts
2. **NSLA-based alerting** which highlights potential abnormalities or indicators of attack
3. **Auditing** through 365-day storage of logs
4. **Event collection** across the estate's devices to ensure improved threat detection
5. **Log collector** tuning which reduces false positives over time, increasing ability to accurately detect anomalous events
6. **Experienced, skilled** human analysis, working to reduce false positives
7. **Advanced incident responders** to mitigate and investigate the root cause of attacks when confirmed security events are declared
8. **Initial application** of 'detect-only' policies to the endpoint management server or appliance followed by fine-tuning
9. **Creating** blacklists and whitelists
10. **Creating or amending** a business' endpoint- or end-user-based policies, followed by monthly fine-tuning
11. **Proactive 24x7x365 monitoring** of key device metrics, and continuous help desk support
12. **Patching** updates and upgrades
13. **Weekly back-ups** of device policies and hardware configuration



Adopting a managed security approach to network and endpoint security will free up other personnel in a company, while ensuring that security practices and policies are always up-to-date. An organisation looking to expand its footprint, for instance, can focus on business growth and international strategy, while an external team manages the increase in endpoints that come with new hires, navigates regional data regulations, and guarantees network defences are global and always-on.

To gain the kind of in-depth, comprehensive, and continuous visibility needed to manage and secure Windows endpoints, we incorporate Microsoft Sysmon into the toolkit. This gives whichever organisation we're working with an invaluable source of insight, whilst taking away the pressures on them of collecting and analysing log sources.

> **Adopting a managed security approach to network and endpoint security will free up other personnel in a company, while ensuring that security practices and policies are always up-to-date.**

As our team's focus is solely on an organisation's network and endpoint security, any breaches or potential criminal activity can be rapidly identified and rectified. Speed is key: the longer an attack goes undetected, the more damage can be caused.

Data breaches and network and endpoint attacks will never completely disappear. And with the burgeoning IoT and upward trend in remote working policies, they'll remain a real and present threat. However, digital transformation and new ways of working should be embraced by organisations as means of improving operations and boosting revenues. Outsourcing services to specialist teams means that cybersecurity will always remain top of a business' agenda without sacrificing its internal resources. As a result, a business can guarantee robust, effective, and agile protection for its customers, employees, and bottom line.

Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to protect freedom and build a safer digital society.

We are threat research, intelligence-driven, offering unparalleled access to current and emerging threats. With a 25+ year track record in information security, 250+ researchers & analysts and 16 SOCs distributed across the world and sales and services support in 160 countries, we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

We embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. It is our people that make us different.

We are proud of our high-end security research unit, thanks to which we publish regularly white papers, articles and tools on cybersecurity which are widely recognised and used throughout the industry and featured at industry conferences including, Infosec, Manchester DTX, RSA, BlackHat and DefCon.

Orange
Cyberdefense

orange™